ceive nonimmigrant students or exchange visitor program participants under section 1101(a)(15)(F), (M), or (J) of title 8, or section 1372 of title 8, as required by section 1762 of title 8; or

(2) been suspended or terminated pursuant to section 1762(c) of title 8.

(Pub. L. 107–305, § 16, Nov. 27, 2002, 116 Stat. 2381.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning Pub. L. 107–305, Nov. 27, 2002, 116 Stat. 2367, known as the Cyber Security Research and Development Act, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7401 of this title and Tables.

§ 7411. Report on grant and fellowship programs

Within 24 months after November 27, 2002, the Director, in consultation with the Assistant to the President for National Security Affairs, shall submit to Congress a report reviewing this chapter to ensure that the programs and fellowships are being awarded under this chapter to individuals and institutions of higher education who are in compliance with the Immigration and Nationality Act (8 U.S.C. 1101 et seq.) in order to protect our national security.

(Pub. L. 107–305, § 17, Nov. 27, 2002, 116 Stat. 2381.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning Pub. L. 107–305, Nov. 27, 2002, 116 Stat. 2367, known as the Cyber Security Research and Development Act, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7401 of this title and Tables.

The Immigration and Nationality Act, referred to in text, is act June 27, 1952, ch. 477, 66 Stat. 163, as amended, which is classified principally to chapter 12 (§ 1101 et seq.) of Title 8, Aliens and Nationality. For complete classification of this Act to the Code, see Short Title note set out under section 1101 of Title 8 and Tables.

CHAPTER 100A—CYBERSECURITY ENHANCEMENT

§ 7421. Definitions

In this chapter:

(1) Cybersecurity mission

The term ''cybersecurity mission'' means activities that encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as such activities relate to the security and stability of cyberspace.

(2) Information system

The term ''information system'' has the meaning given that term in section 3502 of title 44.

(Pub. L. 113–274, § 2, Dec. 18, 2014, 128 Stat. 2971.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning Pub. L. 113–274, Dec. 18, 2014, 128 Stat. 2971, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out below and Tables.

SHORT TITLE

Pub. L. 113–274, § 1(a), Dec. 18, 2014, 128 Stat. 2971, provided that: ''This Act [enacting this chapter and amending sections 272, 278g–3, 7403, and 7406 of this title] may be cited as the 'Cybersecurity Enhancement Act of 2014'.''

§ 7422. No regulatory authority

Nothing in this chapter shall be construed to confer any regulatory authority on any Federal, State, tribal, or local department or agency.

(Pub. L. 113–274, § 3, Dec. 18, 2014, 128 Stat. 2972.)

REFERENCES IN TEXT

This chapter, referred to in text, was in the original ''this Act'', meaning Pub. L. 113–274, Dec. 18, 2014, 128 Stat. 2971, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7421 of this title and Tables.

§ 7423. No additional funds authorized

No additional funds are authorized to carry out this Act, and the amendments made by this Act. This Act, and the amendments made by this Act, shall be carried out using amounts otherwise authorized or appropriated.

(Pub. L. 113–274, § 4, Dec. 18, 2014, 128 Stat. 2972.)

REFERENCES IN TEXT

This Act, and the amendments made by this Act, referred to in text, is Pub. L. 113–274, Dec. 18, 2014, 128 Stat. 2971, which enacted this chapter and amended sections 272, 278g–3, 7403, and 7406 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 7421 of this title and Tables.

SUBCHAPTER I—CYBERSECURITY RESEARCH AND DEVELOPMENT

§ 7431. Federal cybersecurity research and development

(a) Fundamental cybersecurity research

(1) Federal cybersecurity research and development strategic plan

The heads of the applicable agencies and departments, working through the National Science and Technology Council and the Networking and Information Technology Research and Development Program, shall develop and update every 4 years a Federal cybersecurity research and development strategic plan (referred to in this subsection as the ''strategic plan'') based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking systems. The heads of the applicable agencies and departments shall build upon existing programs and plans to develop the strategic plan to meet objectives in cybersecurity, such as—

(A) how to design and build complex software-intensive systems that are secure and reliable when first deployed;

(B) how to test and verify that software and hardware, whether developed locally or obtained from a third party, is free of significant known security flaws;

(C) how to test and verify that software and hardware obtained from a third party correctly implements stated functionality, and only that functionality;

(D) how to guarantee the privacy of an individual, including that individual's identity, information, and lawful transactions when stored in distributed systems or transmitted over networks;

(E) how to build new protocols to enable the Internet to have robust security as one of the key capabilities of the Internet;

(F) how to determine the origin of a message transmitted over the Internet;

(G) how to support privacy in conjunction with improved security;

(H) how to address the problem of insider threats;

(I) how improved consumer education and digital literacy initiatives can address human factors that contribute to cybersecurity;

(J) how to protect information processed, transmitted, or stored using cloud computing or transmitted through wireless services; and

(K) any additional objectives the heads of the applicable agencies and departments, in coordination with the head of any relevant Federal agency and with input from stakeholders, including appropriate national laboratories, industry, and academia, determine appropriate.

(2) Requirements

(A) Contents of plan

The strategic plan shall—

(i) specify and prioritize near-term, mid-term, and long-term research objectives, including objectives associated with the research identified in section 7403(a)(1) of this title;

(ii) specify how the near-term objectives described in clause (i) complement research and development areas in which the private sector is actively engaged;

(iii) describe how the heads of the applicable agencies and departments will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure, and to protect consumer privacy;

(iv) describe how the heads of the applicable agencies and departments will foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the timely benefit of society and the national interest, including through the dissemination of best practices and other outreach activities;

(v) describe how the heads of the applicable agencies and departments will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems; and

(vi) describe how the heads of the applicable agencies and departments will facilitate access by academic researchers to the infrastructure described in clause (v), as well as to relevant data, including event data.

(B) Private sector efforts

In developing, implementing, and updating the strategic plan, the heads of the applicable agencies and departments, working through the National Science and Technology Council and Networking and Information Technology Research and Development Program, shall work in close cooperation with industry, academia, and other interested stakeholders to ensure, to the extent possible, that Federal cybersecurity research and development is not duplicative of private sector efforts.

(C) Recommendations

In developing and updating the strategic plan the heads of the applicable agencies and departments shall solicit recommendations and advice from—

(i) the advisory committee established under section 5511(b)(1) of this title; and

(ii) a wide range of stakeholders, including industry, academia, including representatives of minority serving institutions and community colleges, National Laboratories, and other relevant organizations and institutions.

(D) Implementation roadmap

The heads of the applicable agencies and departments, working through the National Science and Technology Council and Networking and Information Technology Research and Development Program, shall develop and annually update an implementa-

tion roadmap for the strategic plan. The implementation roadmap shall—

(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated;

(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year;

(iii) estimate the funding required for each major research objective of the strategic plan for the following 3 fiscal years; and

(iv) track ongoing and completed Federal cybersecurity research and development projects.

(3) Reports to Congress

The heads of the applicable agencies and departments, working through the National Science and Technology Council and Networking and Information Technology Research and Development Program, shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives—

(A) the strategic plan not later than 1 year after December 18, 2014;

(B) each quadrennial update to the strategic plan; and

(C) the implementation roadmap under subparagraph (D), and its annual updates, which shall be appended to the annual report required under section 5511(a)(2)(D) of this title.

(4) Definition of applicable agencies and departments

In this subsection, the term ''applicable agencies and departments'' means the agencies and departments identified in clauses (i) through (x) of section 5511(a)(3)(B) of this title or designated under clause (xi) of that section.

(b) Cybersecurity practices research

The Director of the National Science Foundation shall support research that—

(1) develops, evaluates, disseminates, and integrates new cybersecurity practices and concepts into the core curriculum of computer science programs and of other programs where graduates of such programs have a substantial probability of developing software after graduation, including new practices and concepts relating to secure coding education and improvement programs; and

(2) develops new models for professional development of faculty in cybersecurity education, including secure coding development.

(c) Cybersecurity modeling and test beds

(1) Review

Not later than 1 year after December 18, 2014, the Director of the National Science Foundation, in coordination with the Director of the Office of Science and Technology Policy, shall conduct a review of cybersecurity test beds in existence on December 18, 2014, to inform the grants under paragraph (2). The review shall include an assessment of whether a sufficient number of cybersecurity test beds are available to meet the research needs under the Federal cybersecurity research and development strategic plan. Upon completion, the Director shall submit the review to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

(2) Additional cybersecurity modeling and test beds

(A) In general

If the Director of the National Science Foundation, after the review under paragraph (1), determines that the research needs under the Federal cybersecurity research and development strategic plan require the establishment of additional cybersecurity test beds, the Director of the National Science Foundation, in coordination with the Secretary of Commerce and the Secretary of Homeland Security, may award grants to institutions of higher education or research and development nonprofit institutions to establish cybersecurity test beds.

(B) Requirement

The cybersecurity test beds under subparagraph (A) shall be sufficiently robust in order to model the scale and complexity of real-time cyber attacks and defenses on real world networks and environments.

(C) Assessment required

The Director of the National Science Foundation, in coordination with the Secretary of Commerce and the Secretary of Homeland Security, shall evaluate the effectiveness of any grants awarded under this subsection in meeting the objectives of the Federal cybersecurity research and development strategic plan not later than 2 years after the review under paragraph (1) of this subsection, and periodically thereafter.

(d) Coordination with other research initiatives

In accordance with the responsibilities under section 5511 of this title, the Director of the Office of Science and Technology Policy shall coordinate, to the extent practicable, Federal research and development activities under this section with other ongoing research and development security-related initiatives, including research being conducted by—

(1) the National Science Foundation;

(2) the National Institute of Standards and Technology;

(3) the Department of Homeland Security;

(4) other Federal agencies;

(5) other Federal and private research laboratories, research entities, and universities;

(6) institutions of higher education;

(7) relevant nonprofit organizations; and

(8) international partners of the United States.

(e) Omitted

(f) Research on the science of cybersecurity

The head of each agency and department identified under section 5511(a)(3)(B) of this title,

through existing programs and activities, shall support research that will lead to the development of a scientific foundation for the field of cybersecurity, including research that increases understanding of the underlying principles of securing complex networked systems, enables repeatable experimentation, and creates quantifiable security metrics.

(Pub. L. 113–274, title II, § 201, Dec. 18, 2014, 128 Stat. 2974.)

CODIFICATION

Section is comprised of section 201 of Pub. L. 113–274. Subsec. (e) of section 201 of Pub. L. 113–274 amended section 7403 of this title.

SUBCHAPTER II—EDUCATION AND WORKFORCE DEVELOPMENT

§ 7441. Cybersecurity competitions and challenges

(a) In general

The Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security, in consultation with the Director of the Office of Personnel Management, shall—

(1) support competitions and challenges under section 3719 of this title (as amended by section 105 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 3989)) or any other provision of law, as appropriate—

(A) to identify, develop, and recruit talented individuals to perform duties relating to the security of information technology in Federal, State, local, and tribal government agencies, and the private sector; or

(B) to stimulate innovation in basic and applied cybersecurity research, technology development, and prototype demonstration that has the potential for application to the information technology activities of the Federal Government; and

(2) ensure the effective operation of the competitions and challenges under this section.

(b) Participation

Participants in the competitions and challenges under subsection (a)(1) may include—

(1) students enrolled in grades 9 through 12;

(2) students enrolled in a postsecondary program of study leading to a baccalaureate degree at an institution of higher education;

(3) students enrolled in a postbaccalaureate program of study at an institution of higher education;

(4) institutions of higher education and research institutions;

(5) veterans; and

(6) other groups or individuals that the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security determine appropriate.

(c) Affiliation and cooperative agreements

Competitions and challenges under this section may be carried out through affiliation and cooperative agreements with—

(1) Federal agencies;

(2) regional, State, or school programs supporting the development of cyber professionals;

(3) State, local, and tribal governments; or

(4) other private sector organizations.

(d) Areas of skill

Competitions and challenges under subsection (a)(1)(A) shall be designed to identify, develop, and recruit exceptional talent relating to—

(1) ethical hacking;

(2) penetration testing;

(3) vulnerability assessment;

(4) continuity of system operations;

(5) security in design;

(6) cyber forensics;

(7) offensive and defensive cyber operations; and

(8) other areas the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security consider necessary to fulfill the cybersecurity mission.

(e) Topics

In selecting topics for competitions and challenges under subsection (a)(1), the Secretary of Commerce, Director of the National Science Foundation, and Secretary of Homeland Security—

(1) shall consult widely both within and outside the Federal Government; and

(2) may empanel advisory committees.

(f) Internships

The Director of the Office of Personnel Management may support, as appropriate, internships or other work experience in the Federal Government to the winners of the competitions and challenges under this section.

(Pub. L. 113–274, title III, § 301, Dec. 18, 2014, 128 Stat. 2981.)

REFERENCES IN TEXT

Section 3719 of this title (as amended by section 105 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 3989)), referred to in subsec. (a)(1), probably means section 3719 of this title as enacted by section 105(a) of Pub. L. 111–358.

§ 7442. Federal Cyber Scholarship-for-Service Program

(a) In general

The Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management and Secretary of Homeland Security, shall continue a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments.

(b) Program description and components

The Federal Cyber Scholarship-for-Service Program shall—

(1) provide scholarships through qualified institutions of higher education, including community colleges, to students who are enrolled in programs of study at institutions of higher education leading to degrees or specialized program certifications in the cybersecurity field;

(2) provide the scholarship recipients with summer internship opportunities or other

meaningful temporary appointments in the Federal information technology workforce; and

(3) prioritize the employment placement of scholarship recipients in the Federal Government.

(c) Scholarship amounts

Each scholarship under subsection (b) shall be in an amount that covers the student's tuition and fees at the institution under subsection (b)(1) for not more than 3 years and provides the student with an additional stipend.

(d) Post-award employment obligations

Each scholarship recipient, as a condition of receiving a scholarship under the program, shall enter into an agreement under which the recipient agrees to work in the cybersecurity mission of a Federal, State, local, or tribal agency for a period equal to the length of the scholarship following receipt of the student's degree.

(e) Hiring authority

(1) Appointment in excepted service

Notwithstanding any provision of chapter 33 of title 5 governing appointments in the competitive service, an agency shall appoint in the excepted service an individual who has completed the eligible degree program for which a scholarship was awarded.

(2) Noncompetitive conversion

Except as provided in paragraph (4), upon fulfillment of the service term, an employee appointed under paragraph (1) may be converted noncompetitively to term, career-conditional or career appointment.

(3) Timing of conversion

An agency may noncompetitively convert a term employee appointed under paragraph (2) to a career-conditional or career appointment before the term appointment expires.

(4) Authority to decline conversion

An agency may decline to make the noncompetitive conversion or appointment under paragraph (2) for cause.

(f) Eligibility

To be eligible to receive a scholarship under this section, an individual shall—

(1) be a citizen or lawful permanent resident of the United States;

(2) demonstrate a commitment to a career in improving the security of information technology;

(3) have demonstrated a high level of proficiency in mathematics, engineering, or computer sciences;

(4) be a full-time student in an eligible degree program at a qualified institution of higher education, as determined by the Director of the National Science Foundation; and

(5) accept the terms of a scholarship under this section.

(g) Conditions of support

(1) In general

As a condition of receiving a scholarship under this section, a recipient shall agree to provide the qualified institution of higher education with annual verifiable documentation of post-award employment and up-to-date contact information.

(2) Terms

A scholarship recipient under this section shall be liable to the United States as provided in subsection (i) if the individual—

(A) fails to maintain an acceptable level of academic standing at the applicable institution of higher education, as determined by the Director of the National Science Foundation;

(B) is dismissed from the applicable institution of higher education for disciplinary reasons;

(C) withdraws from the eligible degree program before completing the program;

(D) declares that the individual does not intend to fulfill the post-award employment obligation under this section; or

(E) fails to fulfill the post-award employment obligation of the individual under this section.

(h) Monitoring compliance

As a condition of participating in the program, a qualified institution of higher education shall—

(1) enter into an agreement with the Director of the National Science Foundation, to monitor the compliance of scholarship recipients with respect to their post-award employment obligations; and

(2) provide to the Director of the National Science Foundation, on an annual basis, the post-award employment documentation required under subsection (g)(1) for scholarship recipients through the completion of their post-award employment obligations.

(i) Amount of repayment

(1) Less than 1 year of service

If a circumstance described in subsection (g)(2) occurs before the completion of 1 year of a post-award employment obligation under this section, the total amount of scholarship awards received by the individual under this section shall—

(A) be repaid; or

(B) be treated as a loan to be repaid in accordance with subsection (j).

(2) 1 or more years of service

If a circumstance described in subparagraph (D) or (E) of subsection (g)(2) occurs after the completion of 1 or more years of a post-award employment obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall—

(A) be repaid; or

(B) be treated as a loan to be repaid in accordance with subsection (j).

(j) Repayments

A loan described subsection (i) shall—

(1) be treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher Education Act of 1965 (20 U.S.C. 1087a et seq.); and

(2) be subject to repayment, together with interest thereon accruing from the date of the scholarship award, in accordance with terms and conditions specified by the Director of the National Science Foundation (in consultation with the Secretary of Education) in regulations promulgated to carry out this subsection.

(k) Collection of repayment

(1) In general

In the event that a scholarship recipient is required to repay the scholarship award under this section, the qualified institution of higher education providing the scholarship shall—

(A) determine the repayment amounts and notify the recipient and the Director of the National Science Foundation of the amounts owed; and

(B) collect the repayment amounts within a period of time as determined by the Director of the National Science Foundation, or the repayment amounts shall be treated as a loan in accordance with subsection (j).

(2) Returned to Treasury

Except as provided in paragraph (3), any repayment under this subsection shall be returned to the Treasury of the United States.

(3) Retain percentage

A qualified institution of higher education may retain a percentage of any repayment the institution collects under this subsection to defray administrative costs associated with the collection. The Director of the National Science Foundation shall establish a single, fixed percentage that will apply to all eligible entities.

***(l)* Exceptions**

The Director of the National Science Foundation may provide for the partial or total waiver or suspension of any service or payment obligation by an individual under this section whenever compliance by the individual with the obligation is impossible or would involve extreme hardship to the individual, or if enforcement of such obligation with respect to the individual would be unconscionable.

(m) Evaluation and report

The Director of the National Science Foundation shall evaluate and report periodically to Congress on the success of recruiting individuals for scholarships under this section and on hiring and retaining those individuals in the public sector workforce.

(Pub. L. 113–274, title III, § 302, Dec. 18, 2014, 128 Stat. 2982.)

REFERENCES IN TEXT

The Higher Education Act of 1965, referred to in subsec. (j)(1), is Pub. L. 89–329, Nov. 8, 1965, 79 Stat. 1219. Part D of title IV of the Act is classified to part C (§ 1087a et seq.) of subchapter IV of chapter 28 of Title 20, Education. For complete classification of this Act to the Code, see Short Title note set out under section 1001 of Title 20 and Tables.

SUBCHAPTER III—CYBERSECURITY AWARENESS AND PREPAREDNESS

§ 7451. National cybersecurity awareness and education program

(a) National cybersecurity awareness and education program

The Director of the National Institute of Standards and Technology (referred to in this section as the ''Director''), in consultation with appropriate Federal agencies, industry, educational institutions, National Laboratories, the Networking and Information Technology Research and Development program, and other organizations shall continue to coordinate a national cybersecurity awareness and education program, that includes activities such as—

(1) the widespread dissemination of cybersecurity technical standards and best practices identified by the Director;

(2) efforts to make cybersecurity best practices usable by individuals, small to medium-sized businesses, educational institutions, and State, local, and tribal governments;

(3) increasing public awareness of cybersecurity, cyber safety, and cyber ethics;

(4) increasing the understanding of State, local, and tribal governments, institutions of higher education, and private sector entities of—

(A) the benefits of ensuring effective risk management of information technology versus the costs of failure to do so; and

(B) the methods to mitigate and remediate vulnerabilities;

(5) supporting formal cybersecurity education programs at all education levels to prepare and improve a skilled cybersecurity and computer science workforce for the private sector and Federal, State, local, and tribal government; and

(6) promoting initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal Government and develop strategies for recruitment, training, and retention.

(b) Considerations

In carrying out the authority described in subsection (a), the Director, in consultation with appropriate Federal agencies, shall leverage existing programs designed to inform the public of safety and security of products or services, including self-certifications and independently verified assessments regarding the quantification and valuation of information security risk.

(c) Strategic plan

The Director, in cooperation with relevant Federal agencies and other stakeholders, shall build upon programs and plans in effect as of December 18, 2014, to develop and implement a strategic plan to guide Federal programs and activities in support of the national cybersecurity awareness and education program under subsection (a).

(d) Report

Not later than 1 year after December 18, 2014, and every 5 years thereafter, the Director shall transmit the strategic plan under subsection (c) to the Committee on Commerce, Science, and

Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

(Pub. L. 113–274, title IV, § 401, Dec. 18, 2014, 128 Stat. 2985.)

SUBCHAPTER IV—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

§ 7461. Definitions

In this subchapter:

(1) Director

The term ''Director'' means the Director of the National Institute of Standards and Technology.

(2) Institute

The term ''Institute'' means the National Institute of Standards and Technology.

(Pub. L. 113–274, title V, § 501, Dec. 18, 2014, 128 Stat. 2986.)

§ 7462. International cybersecurity technical standards

(a) In general

The Director, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after December 18, 2014, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) Consultation with the private sector

In carrying out the activities specified in subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

(Pub. L. 113–274, title V, § 502, Dec. 18, 2014, 128 Stat. 2986.)

§ 7463. Cloud computing strategy

(a) In general

The Director, in coordination with the Office of Management and Budget, in collaboration with the Federal Chief Information Officers Council, and in consultation with other relevant Federal agencies and stakeholders from the private sector, shall continue to develop and encourage the implementation of a comprehensive strategy for the use and adoption of cloud computing services by the Federal Government.

(b) Activities

In carrying out the strategy described under subsection (a), the Director shall give consideration to activities that—

(1) accelerate the development, in collaboration with the private sector, of standards that address interoperability and portability of cloud computing services;

(2) advance the development of conformance testing performed by the private sector in support of cloud computing standardization; and

(3) support, in coordination with the Office of Management and Budget, and in consultation with the private sector, the development of appropriate security frameworks and reference materials, and the identification of best practices, for use by Federal agencies to address security and privacy requirements to enable the use and adoption of cloud computing services, including activities—

(A) to ensure the physical security of cloud computing data centers and the data stored in such centers;

(B) to ensure secure access to the data stored in cloud computing data centers;

(C) to develop security standards as required under section 278g–3 of this title; and

(D) to support the development of the automation of continuous monitoring systems.

(Pub. L. 113–274, title V, § 503, Dec. 18, 2014, 128 Stat. 2986.)

§ 7464. Identity management research and development

The Director shall continue a program to support the development of voluntary and cost-effective technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

(Pub. L. 113–274, title V, § 504, Dec. 18, 2014, 128 Stat. 2987.)

CHAPTER 101—NANOTECHNOLOGY RESEARCH AND DEVELOPMENT

Sec.

§ 7501. National Nanotechnology Program

(a) National Nanotechnology Program

The President shall implement a National Nanotechnology Program. Through appropriate agencies, councils, and the National Nanotechnology Coordination Office established in section 7502 of this title, the Program shall—

(1) establish the goals, priorities, and metrics for evaluation for Federal nanotechnology research, development, and other activities;

(2) invest in Federal research and development programs in nanotechnology and related sciences to achieve those goals; and

(3) provide for interagency coordination of Federal nanotechnology research, development, and other activities undertaken pursuant to the Program.